



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/051,668	01/17/2002	Patrick L. Connor	PW 0249740 P12832	1163

7590

12/21/2005

Pillsbury Winthrop LLP
Intellectual Property Group
Suite 2800
725 South Figueroa Street
Los Angeles, CA 90017-5406

EXAMINER

PATEL, NIRAV B

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 12/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

DETAILED ACTION

1. Applicant's amendment filed on November 14, 2005 has been entered.
2. Claims 1-5, 8-13, 16, 18, 19, 21, 22, 24, 25, 27-30 are pending. Claims 6, 7, 14, 15, 17, 20, 23, 26 and 31 are cancelled by the applicant and claims 1, 8, 16, 22 and 28 are also amended by the applicant.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-5, 8-13, 16, 18, 19, 21, 22, 24, 25, 27-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishna, Suresh (WO 01/05086) and in view of Johnson et al (US Patent No. 6,754,755).

As per claim 1, Krishna discloses:

a network to transmit an encrypted packet; and a computer to receive said encrypted packet from said network, and to perform a decryption operation thereupon to convert said encrypted packet to a decrypted packet [**page 3 line 8 “as connecting a single computer to a WAN, to large corporate network”, line 6 “to efficiently process encryption/decryption of data packets”**], said computer including:

Art Unit: 2135

a network interface to provide electronic communication between said computer and said network **[Fig. 1A component 112 Network Interface]**, a network driver to regulate said decryption operation **[page 3 lines 7-9 “Cryptography acceleration chip in accordance as diverse as connecting a single computer to a WAN”]**, a controller to perform said decryption operation **[page 3 lines 5-6 “a plurality of cryptography engines and includes a classification engine configured to efficiently process encryption/decryption of data packets”]**, a host memory to store data that is used or generated by said decryption operation **[Fig. 1B component 166 Main Memory page 7 line 36, page 8 lines 1-2 “the processed packets are then sent back over the matrix 154, through the memory 166”]**, and a bus providing electronic communication among said network interface, said network driver, said host memory and said controller **[Fig. 1A component 104 system bus]**.

Krishna doesn't expressively mention that asserting an interrupt prior to a complete transfer (i.e. early interrupt) of said decrypted packet from said controller to said host memory wherein said controller asserts an additional interrupt after completion of said decryption operation, and said network driver specifies an average latency value to said controller for use in said decryption operation (i.e. to determine when a interrupt should be asserted or how long before completing transfer of a decrypted packet back to host memory).

However, Johnson teaches that asserting *an interrupt prior to a complete transfer (i.e. early interrupt)* of said decrypted packet from said controller to said host memory **[col. 9 lines 22-38 “the interrupt logic 320 of the NIC 260 to assert the**

Art Unit: 2135

interrupt early by the approximate latency period” Fig. 3] wherein said controller asserts an additional *interrupt after completion of* said decryption operation **[col. 8 lines 51-53, Fig. 3, 5]**, and said network driver *specifies an average latency value* to said controller for use in said decryption operation (i.e. to determine when a interrupt should be asserted or how long before completing transfer of a decrypted packet back to host memory) **[col. 9 lines 22-38, Fig. 5, 6]**.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Johnson into the teaching of Krishna to assert the interrupt and control occurrence of the interrupt. The modification would be obvious because one of ordinary skill in the art would be motivated to reduce process overhead, thereby improve overall system efficiency. In addition, to improve the network traffic flow and to increase the bandwidth **[Johnson, col. 13 lines 18-24,30-33]**.

As per claim 2, the rejection of claim 1 is incorporated and further Krishna discloses:

security association (SA) is stored in said host memory **[page 11 lines 8-10 “the chip also includes various buffers 210 for storing packet data, security association information” Fig. 3]**.

As per claim 3, the rejection of claim 2 is incorporated and further Krishna discloses:

Art Unit: 2135

network driver parses said encrypted packet, matches said encrypted packet with one of said at least one SA [**page 11 lines 18-20 “packet header information is sent to a packet classifier unit 204 where a classification engine rapidly determines security association information required for processing the packet”**] and instructs said network interface to transfer said encrypted packet and said one SA across said bus to said controller [**page 11 lines 31-33 “the packet distributor unit 306 then distributes the security association information(SA) received from the packet classifier unit 304 and the packet data via the internal bus 305 among a plurality of cryptography processing engines 316” Fig. 6A**].

As per claim 4, the rejection of claim 1 is incorporated and further Krishna discloses:

network interface includes a cryptography accelerator [**page 6 lines 16-17 “as shown in Fig. 1, the cryptography acceleration chip 102 may be part of an otherwise standard network line card 103 which includes a WAN interface 112”**].

As per claim 5, the rejection of claim 1 is incorporated and further Krishna discloses:

controller transfers said decrypted packet across said bus from said controller to said host memory [**page 7 line 36, page 8 line 1 “the processed packet are then sent back over the matrix 154, through the memory 166”**].

As per claim 8, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

As per claim 9, the rejection of claim 8 is incorporated and further Krishna teaches:

network interface to provide electronic communication between said computer and a network **[page 6 lines 16-18 “as shown in Fig. 1, the cryptography acceleration chip 102 may be part of an otherwise standard network line card 103 which includes a WAN interface 112 that connects the processing system 100 to a WAN, such as the internet”]**.

As per claim 10, the rejection of claim 9 is incorporated and is rejected for the same reason set forth in the rejection of claim 2 above.

As per claim 11, the rejection of claim 10 is incorporated and is rejected for the same reason set forth in the rejection of claim 3 above.

As per claim 12, the rejection of claim 8 is incorporated and is rejected for the same reason set forth in the rejection of claim 4 above.

As per claim 13, the rejection of claim 8 is incorporated and is rejected for the same reason set forth in the rejection of claim 5 above.

As per claim 16, Krishna teaches:

receiving said encrypted packet from a network **[page 3 lines 6-9]**;
issuing a decryption command to a controller **[page 12 lines 5-6 “the packet distributor unit 306 includes a processor which control the sequencing and processing of the packets according to microcode stored on the chip” Fig. 3]**;
converting said encrypted packet to a decrypted packet **[page 3 lines 5-6]**;
transferring said decrypted packet to a host **[Fig. 1B component 166 Main Memory page 7 line 36, page 8 lines 1-2]**;

Krishna doesn't expressively mention that determining a time for said assertion of said interrupt in response to said decryption command; asserting an interrupt at a time before completing said transfer of said decrypted packet to said host memory, and asserting an additional interrupt upon completion of said transfer of said decrypted packet to said host memory.

However, Johnson teaches that *determining a time* for said assertion of said interrupt in response to said decryption command **[col. 9 lines 22-38 “ to determine an approximate interrupt latency period of the computer system 102 on the network 100 and cause the interrupt logic 320 of the NIC 260 to assert the interrupt”, Fig. 5, 6]**; asserting an *interrupt at a time before* (i.e. early interrupt) completing said transfer of said decrypted packet to said host memory **[col. 9 lines 22-38 “the interrupt logic 320 of the NIC 260 to assert the interrupt early by the approximate latency period” Fig. 3]** and *asserting an additional interrupt* upon completion of said transfer of said decrypted packet to said host memory **[col. 8 lines**

Art Unit: 2135

51-53, Fig. 3, 5 “a message is being transferred or after the message is transferred from the NIC 260 to the system memory 206, the interrupt logic 320 of the NIC 260 generates an interrupt”].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the teaching of Johnson into the teaching of Krishna to assert the interrupt and control occurrence of the interrupt. The modification would be obvious because one of ordinary skill in the art would be motivated to reduce process overhead, thereby improve overall system efficiency. In addition, to improve the network traffic flow and to increase the bandwidth **[Johnson, col. 13 lines 18-24,30-33]**.

As per claim 18, the rejection of claim 16 is incorporated and further claim 18 is a method claim corresponds to system claim 3 and is rejected for the same reason set forth in the rejection of claim 3 above.

As per claim 19, the rejection of claim 16 is incorporated and further Krishna teaches:
step of converting said encrypted packet to said decrypted packet further includes authenticating said decrypted packet **[Fig. 6A page 9 lines 9-10 “then pass the packet along to one of the four cryptography and authentication engines 214”]**.

Art Unit: 2135

As per claim 21, the rejection of claim 16 is incorporated and further Krishna teaches:

decrypted packet to a protocol stack after asserting said interrupt **[Fig. 3 component 318 output FIFO (MAC) *page 12 lines 16-17* “the packet distributor 306 control the output FIFO 318 to ensure that packet ordering (i.e. Per-flow ording) is maintained”, *page 9 lines 31-35* “Per-flow ordering offers a good trade-off between maximizing end-to-end system performance (specifically desktop PC TCP/IP stack)”]**.

As per claim 22, it is a device claim corresponds to method claim 16 and is rejected for the same reason set forth in the rejection of claim 16 above. Further Krishna teaches:

a machine-readable storage medium; and machine-readable program code, stored on the machine-readable storage medium **[*page 12 lines 5-6* “a processor which controls the sequencing and processing of the packets according to microcode stored on the chip”]**.

As per claim 24, the rejection of claim 22 is incorporated and further claim 24 is a device claim corresponds to system claim 3 and is rejected for the same reason set forth in the rejection of claim 3 above.

As per claim 25, the rejection of claim 22 is incorporated and further claim 25 is a device claim corresponds to method claim 19 and is rejected for the same reason set forth in the rejection of claim 19 above.

As per claim 27, the rejection of claim 22 is incorporated and further claim 27 is a device claim corresponds to method claim 21 and is rejected for the same reason set forth in the rejection of claim 21 above.

As per claim 28, it encompasses limitations that are similar to limitations of claim 1. Thus, it is rejected with the same rationale applied against claim 1 above.

As per claim 29, the rejection of claim 28 is incorporated and further claim 29 is corresponds to claim 2 and is rejected for the same reason set forth in the rejection of claim 2 above.

As per claim 30, the rejection of claim 29 is incorporated and further claim 30 is corresponds to claim 3 and is rejected for the same reason set forth in the rejection of claim 3 above.

Response to Amendment

4. Applicant's amendment filed on November 14, 2005 has been fully considered and is persuasive. Therefore, previous rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is based on Krishna, Suresh (WO 01/05086) and Johnson et al (US Patent No. 6,754,755). See rejections above.

Conclusion

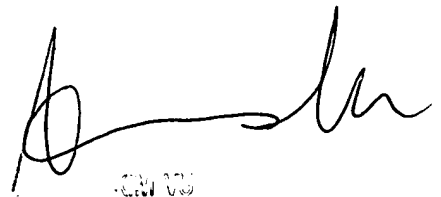
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. The examiner can normally be reached on 8 am - 4:30 pm (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NBP

12/16/05



DEC 16 2005
PATENT EXAMINER
EBC CENTER 2135